IN THE CLAIMS

1. (*Currently amended*) A method for providing access control management to electronic data, the method comprising:

establishing a secured link with a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;

authenticating the user according to the identifier; and

activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

2. (*Original*) The method as recited in Claim 1 further comprising maintaining an access control management, wherein the access control management comprises:

a rule manager including at least one set of rules for the electronic data; and

an administration interface from which the rules for a designated place for the electronic data are created, managed, or updated.

3. (*Previous amended*) The method as recited in Claim 2, wherein the designated place is a folder and all files in the folder are subject to the rules.

4. (*Previous amended*) The method as recited in Claim 2, wherein the designated place is a repository and all files in the repository are subject to the rules.

5. (*Previously amended*) The method as recited in Claim 2, wherein the rule manager provides a graphic user interface from which the rules can be created, managed or updated.

6. (*Previously amended*) The method as recited in Claim 5, wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language.

7. (*Previously amended*) The method as recited in Claim 6, wherein the parameters expressed in the markup language are uploaded to the client machine after the user is authenticated.

8. (*Previously amended*) The method as recited in Claim 7, wherein the markup language is Extensible Access Control Markup Language.

9. (*Original*) The method as recited in Claim 7, wherein the markup language is selected from a group consisting of HTML, XML and SGML.

10. (*Original*) The method as recited in Claim 2, wherein the access control management further comprises a user manager coupled to a database including a list of authorized users and respective access privileges associated with each of the authorized users.

11. (*Original*) The method as recited in Claim 10, wherein the authenticating of the user comprises:

looking up in the database for the user; and

getting, from the database, access location information as to where the user is authorized to access the electronic data if information about the user is located in the database.

12. (*Original*) The method as recited in Claim 11, wherein the identifier further identifiers the client machine; and wherein the authenticating of the user comprises determining, from the access location information, whether the client machine is permitted by the user to access the electronic data.

13. (*Previously amended*) The method as recited in Claim 11, wherein the access location information pertains to locations or specific client machines from which the user is authorized to access the electronic data.

14. (*Original*) The method as recited in Claim 1, wherein the user key is in the client machine; and wherein the activating of the user key comprises:
sending an authentication message to the client machine; and
activating the user key with the authentication message.

15. (*Previously amended*) The method as recited in Claim 14, wherein the electronic data, when secured, includes a header that further includes the security information being encrypted and a signature signifying that the electronic data is secured.

16. (*Cancelled*)

17. (*Original*) The method as recited in Claim 1 further comprising associating the activated user key with the user locally.

18. (*Previously amended*) The method as recited in Claim 17, wherein the electronic data, when secured, includes a header that includes the security information being encrypted and a signature signifying that the electronic data is secured; the encrypted security information including the access rules and a file key, and wherein the method further comprises:
receiving the header from the client machine;
decrypting the security information in the header to retrieve the access rules therein; and
retrieving the file key when the access rules are measured successfully against access privilege of the user.

19. (*Original*) The method as recited in Claim 18 further comprising sending the file key to the client machine in which the encrypted data portion can be decrypted with the file key by a cipher module executing in the client machine.

20. (*Previously amended*) A method for providing access control management to electronic data, the method comprising:

authenticating a user attempting to access the electronic data;

maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when and where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme;

encrypting the security information with the public key when the electronic data is to be written into a store; and

decrypting the security information with the private key when the electronic data is to be accessed by an application.

21. (*Previously amended*) The method as recited in Claim 20, wherein the authentication of the user comprises:

establishing a link with a client machine from which the user is attempting to access the electronic data;

demanding credential information from the user; and

receiving the credential information from the client machine over the link.

22. (*Original*) The method as recited in Claim 21, wherein the credential information includes a pair of username and password provided by the user.

23. (*Original*) The method as recited in Claim 21, wherein the credential information includes biometric information captured from the user by an apparatus coupled to the client machine.

24. (*Previously amended*) The method as recited in Claim 21, wherein the encrypting of the security information with the public key comprises:

receiving access rules and a file key, wherein the file key has been used to produce the encrypted data portion in the client machine;

including the access rules and the file key into the security information; and

encrypting the security information with the public key.

25. (*Original*) The method as recited in Claim 24 further comprising:

generating the header with the security information encrypted therein; and

uploading the header to the client machine where the header is integrated with the encrypted data portion.

26. (*Original*) The method as recited in Claim 24, wherein the access rules are expressed in a markup language.

27. (*Original*) The method as recited in Claim 26, wherein the markup language is one of Extensible Access Control Markup Language, HTML, XML and SGML.

28. (*Original*) The method as recited in Claim 21, wherein the decrypting of the security information with the private key comprises:

receiving the header from the client machine over the link;

parsing the security information from the header; and

decrypting the security information with the private key.

29. (*Original*) The method as recited in Claim 28 further comprising:

obtaining access rules from the security information;

determining whether the access rules accommodate access privilege of the user;

when the determining succeeds,

retrieving a file key from the security information; and

sending the file key to the client machine over the link.

when the determining fails,

sending an error message to the client machine over the link.

30. (*Currently amended*) The method as recited in Claim 29, wherein the error message indicates that the user does not have the access privilege to access the electronic data.

31. (*Currently amended*) A method for providing access control management to electronic data, the method comprising:

receiving a request to access the electronic data;

determining security nature of the electronic data;

when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme,

determining from the security information if the user has necessary access privilege to access the encrypted data portion without consulting with another machine; and

obtaining a file key and decrypting the encrypted data portion with the file key only after the user is determined to have the necessary access privilege to access the encrypted data portion.

32. (*Original*) The method as recited in Claim 31 further comprising retrieving a user key associated with a user making the request.

33. (*Original*) The method as recited in Claim 32 wherein said determining from the security information if the user has necessary access privilege comprises:

decrypting the security information with the user key;

retrieving access rules from the security information; and

measuring the access rules against the access privilege of the user.

34. (*Original*) The method as recited in Claim 33 further comprising:
retrieving ~~a~~ the file key from the security information if the measuring of the access rules against the access privilege succeeds.

35. (*Original*) The method as recited in Claim 33 further comprising:
causing the client machine to display an error message to the user if the measuring of the access rules against the access privilege fails.

36. (*Currently amended*) The method as recited in Claim 32, wherein the retrieving of the user key comprises:
establishing a link with a server executing an access control management;
sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user;
forwarding the header to the server; and
receiving ~~a~~ the file key retrieved from the header.

37. (*Original*) The method as recited in Claim 36 further comprising:
activating a cipher module; and
decrypting the encrypted data portion by the cipher module with the received file key.

38. (*Original*) The method as recited in Claim 37 further comprising loading the decrypted data portion into the application.

39. (*Original*) The method as recited in Claim 32, wherein the retrieving of the user key comprises:
establishing a link with a server executing an access control management;
sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user;
receiving an authentication message after the user is authenticated; and

activating the user key locally in the client machine.

40. (*Original*) The method as recited in Claim 39, wherein the user key is in an illegible format before the activating of the user key locally in the client machine.

41. (*Currently amended*) A system for providing access control management to electronic data, the method comprising:

a client machine executing a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data,

an access control server coupled to the client machine over a network, the access control server including an account manager managing all users who access the electronic data; and

wherein the client machine and a user thereof are caused by the document securing module to be authenticated with the access control server when the security nature indicates that the electronic data is secured; and

wherein access rules in the secured electronic data are retrieved with a user key associated with the user to test against access privilege of the user to determine if the user can access the secured electronic data.

B4

42. (*Currently amended*) The system as recited in Claim 41, wherein the access ~~rules are measured against access~~ privilege of the user is also tested against other rules imposed by the system.

43. (*Currently amended*) The system as recited in Claim 412, wherein the document securing module activates a cipher module to decrypt an encrypted data portion in the secured electronic data with a file key obtained therefrom after the document securing module determines that the access privilege of the user is permitted by the access rules.

44. (*Previously amended*) The system as recited in Claim 43, wherein the user key stays in the access control server that receives part of the secured electronic data; and wherein the access rules and the file key are obtained from the part of the secured electronic data

45. (*Previously amended*) The system as recited in Claim 44, wherein the access control server forwards the file key to the client machine in a secured form over the network.

46. (*Previously amended*) The system as recited in Claim 43, wherein the user key stays in the client machine and is activated when both the client machine and the user are authenticated by the access control server.

47. (*Previously amended*) A system for providing access control management to electronic data, the method comprising:

a storage device including at least an active place designated for keeping the electronic data secured, the secured electronic data including encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data;

a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place;

an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated;

wherein the set of access rules are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode.

48. (*Currently amended*) A software product to be executable in a computing device for providing access control management to electronic data, the software product comprising:

program code for establishing a secured link with a client machine when an authentication request is received therefrom, the authentication request including an identifier identifying a user from the client machine to access the electronic data in a secured format including a file key and security information and an encrypted data, the security information including access rules and controlling restrictive access to the encrypted data portion;

program code for authenticating the user according to the identifier; and

program code for activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

49. (*Previously amended*) The software product as recited in Claim 48 further comprising program code for maintaining an access control management, wherein the access control management comprises:

a rule manager including at least one set of rules for the electronic data; and

an administration interface from which the rules for a designated place for the electronic data are created, managed or updated.

50. (*Previously amended*) The software product as recited in Claim 49, wherein the designated place is a folder and all files in the folder are subject to the rules.

51. (*Previously amended*) The software product as recited in Claim 47, wherein the designated place is a repository and all files in the repository are subject to the rules.

52. (*Previously amended*) The software product as recited in Claim 47, wherein the rule manager provides a graphic user interface from which the rules can be created, managed or updated.

53. (*Previously amended*) The software product as recited in Claim 52, wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language.

54. (*Previously amended*) The software product as recited in Claim 53, wherein the parameters expressed in the markup language are uploaded to the client machine after the authenticating of the user succeeds.

55. (*Previously amended*) The software product as recited in Claim 54, wherein the markup language is Extensible Access Control Markup Language.

56. (*Original*) The software product as recited in Claim 54, wherein the markup language is selected from a group consisting of HTML, XML and SGML.

57. (*Original*) The software product as recited in Claim 49, wherein the access control management further comprises a user manager coupled to a database including a list of authorized users and respective access privileges associated with each of the authorized users.

58. (*Original*) The software product as recited in Claim 57, wherein the program code for authenticating the user comprises:

program code for looking up in the database for the user; and

program code for getting, from the database, access location information as to where the user is authorized to access the electronic data if the user is located in the database.

59. (*Original*) The software product as recited in Claim 58, wherein the identifier further identifiers the client machine; and wherein the program code for authenticating the user comprises program code for determining, from the access location information, whether the client machine is permitted by the user to access the electronic data.

60. (*Previously amended*) The software product as recited in Claim 58, wherein the access location information pertains to locations or specific client machines from which the user is authorized to access the electronic data.

61. (*Original*) The software product as recited in Claim 48, wherein the user key is in the client machine; and wherein the program code for activating the user key comprises:
program code for sending an authentication message to the client machine; and
program code for activating the user key with the authentication message.

62. (*Original*) The software product as recited in Claim 61, wherein the electronic data, when secured, includes a header and an encrypted data portion; and wherein the header includes security information that can be accessed with the activated user key.

63. (*Cancelled*)

64. (*Original*) The software product as recited in Claim 48 further comprising program code for associating the activated user key with the user locally.

65. (*Original*) The software product as recited in Claim 64, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header includes security information and a file key; and wherein the software product further comprises:
program code for receiving the header from the client machine;
program code for decrypting the header to retrieve access rules in the security Information; and

program code for retrieving the file key when the access rules are measured successfully against access privilege of the user.

66. (*Original*) The software product as recited in Claim 65 further comprising sending the file key to the client machine in which the encrypted data portion can be decrypted with the file key by a cipher module executing in the client machine.

67. (*Currently amended*) A software product to be executable in a computing device for providing access control management to electronic data, the software product comprising:

program code for authenticating a user attempting to access the electronic data;

program code for maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling restrictive access to the encrypted data portion and protecting the private key ~~and a public key~~ by access rules therein;

program code for encrypting the security information with the public key when the electronic data is to be written into a store; and

program code for decrypting the security information with the private key when the electronic data is to be accessed by an application.

68. (*Original*) The software product as recited in Claim 67, wherein the program code for authenticating the user comprises:

program code for establishing a link with a client machine from which the user is attempting to access the electronic data;

program code for demanding credential information from the user; and

program code for receiving the credential information from the client machine over the secured link.

69. (*Original*) The software product as recited in Claim 68, wherein the credential information includes a pair of username and password provided by the user.

70. (*Original*) The software product as recited in Claim 68, wherein the credential information includes biometric information captured from the user by an apparatus coupled to the client machine.

71. (*Previously amended*) The software product as recited in Claim 68, wherein the program code for encrypting the security information with the public key comprises:

program code for receiving the access rules and a file key from the client machine over the link, wherein the file key has been used to produce the encrypted data portion in the client machine;

program code for including the access rules and a file key into the security information; and

program code for encrypting the security information with the public key.

72. (*Original*) The software product as recited in Claim 71 further comprising:

program code for generating the header with the security information encrypted therein; and

program code for uploading the header to the client machine where the header is integrated with the encrypted data portion.

73. (*Original*) The software product as recited in Claim 74, wherein the access rules are expressed in a markup language.

74. (*Original*) The software product as recited in Claim 73, wherein the markup language is one of Extensible Access Control Markup Language, HTML, XML and SGML.

75. (*Original*) The software product as recited in Claim 68, wherein the program code for decrypting the security information with the private key comprises:

program code for receiving the header from the client machine over the link;

program code for parsing the security information from the header; and

program code for decrypting the security information with the private key.

76. (*Original*) The software product as recited in Claim 75 further comprising:
program code for obtaining access rules from the security information;
program code for determining whether the access rules accommodate access privilege of the user;
when the determining program code is executed successfully,
program code for retrieving a file from the security information; and
program code for sending the file key to the client machine over the link.
when the determining program code is executed unsuccessfully,
program code for sending an error message to the client machine over the link.

77. (*Original*) The software product as recited in Claim 76 wherein the error message indicate that the user does not have the access privilege to access the electronic data.

---

78. (*Currently amended*) A software product to be executable in a computing device for providing access control management to electronic data, the software product comprising:
program code for receiving a request to access the electronic data;
program code for determining security nature of the electronic data;
when the security nature indicates that the electronic data is secured, wherein the electronic data including a header and an encrypted data portion, the header including security information and the encrypted data portion is an encrypted version of the electronic data according to a predetermined encryption scheme,
program code for determining from the security information if the user has necessary access privilege to access the encrypted data portion; and
program code for a file key from the security information and decrypting the encrypted data portion only after the access privilege of the user is permitted in view of the security information.

---

79. (*Original*) The software product as recited in Claim 78 further comprising program code for retrieving a user key associated with a user making the request.

80. (*Original*) The software product as recited in Claim 79 wherein the program code for determining from the security information, if the user has necessary access privilege, comprises:

program code for decrypting the security information with the user key;

program code for retrieving access rules from the security information; and

program code for measuring the access rules against the access privilege of the user.

81. (*Cancelled*)

82. (*Original*) The software product as recited in Claim 80 further comprising:

program code for causing the client machine to display an error message to the user if the measuring of the access rules against the access privilege fails.

83. (*Original*) The software product as recited in Claim 80, wherein the program code for retrieving the user key comprises:

program code for establishing a link with a server executing an access control management;

program code for sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user;

program code for forwarding the header to the server; and

program code for receiving a file key retrieved from the header.

84. (*Original*) The software product as recited in Claim 83 further comprising:

program code for activating a cipher module; and

program code for decrypting the encrypted data portion by the cipher module with the received file key.

85. (*Original*) The software product as recited in Claim 84 further comprising program code for loading the decrypted data portion into the application.

86. (*Original*) The software product as recited in Claim 79, wherein the program code for retrieving the user key comprises:

program code for establishing a link with a server executing an access control management;

program code for sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user;

program code for receiving an authentication message after the user is authenticated; and

program code for activating the user key locally in the client machine.

87. (*Original*) The software product as recited in Claim 86, wherein the user key is in an illegible format before the activating of the user key locally in the client machine.

88. (*Original*) The software product as recited in Claim 86, wherein the computing device is a media player having a network capacity, the media player generating audio and/or video from the electronic data when the software product is executed in the media player.